

**(9) National Coordinator**

The term “National Coordinator” means the head of the Office of the National Coordinator for Health Information Technology established under section 300jj–11(a) of this title, as added by section 13101.<sup>2</sup>

**(10) Payment**

The term “payment” has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

**(11) Personal health record**

The term “personal health record” means an electronic record of PHR identifiable health information (as defined in section 17937(f)(2) of this title) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

**(12) Protected health information**

The term “protected health information” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

**(13) Secretary**

The term “Secretary” means the Secretary of Health and Human Services.

**(14) Security**

The term “security” has the meaning given such term in section 164.304 of title 45, Code of Federal Regulations.

**(15) State**

The term “State” means each of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

**(16) Treatment**

The term “treatment” has the meaning given such term in section 164.501 of title 45, Code of Federal Regulations.

**(17) Use**

The term “use” has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

**(18) Vendor of personal health records**

The term “vendor of personal health records” means an entity, other than a covered entity (as defined in paragraph (3)), that offers or maintains a personal health record.

(Pub. L. 111–5, div. A, title XIII, §13400, Feb. 17, 2009, 123 Stat. 258.)

## REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

Section 13101, referred to in par. (9), means section 13101 of div. A of Pub. L. 111–5.

<sup>2</sup> See References in Text note below.

## PART A—IMPROVED PRIVACY PROVISIONS AND SECURITY PROVISIONS

**§ 17931. Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions****(a) Application of security provisions**

Sections 164.308, 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations, shall apply to a business associate of a covered entity in the same manner that such sections apply to the covered entity. The additional requirements of this title<sup>1</sup> that relate to security and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

**(b) Application of civil and criminal penalties**

In the case of a business associate that violates any security provision specified in subsection (a), sections 1320d–5 and 1320d–6 of this title shall apply to the business associate with respect to such violation in the same manner such sections apply to a covered entity that violates such security provision.

**(c) Annual guidance**

For the first year beginning after February 17, 2009, and annually thereafter, the Secretary of Health and Human Services shall, after consultation with stakeholders, annually issue guidance on the most effective and appropriate technical safeguards for use in carrying out the sections referred to in subsection (a) and the security standards in subpart C of part 164 of title 45, Code of Federal Regulations, including the use of standards developed under section 300jj–12(b)(2)(B)(vi) of this title, as added by section 13101 of this Act, as such provisions are in effect as of the date before February 17, 2009.<sup>2</sup>

(Pub. L. 111–5, div. A, title XIII, §13401, Feb. 17, 2009, 123 Stat. 260.)

## REFERENCES IN TEXT

This title, referred to in subsec. (a), is title XIII of div. A of Pub. L. 111–5, which enacted this chapter and subchapter XXVIII (§300jj et seq.) of chapter 6A this title, amended sections 1320d, 1320d–5, and 1320d–6 of this title, and enacted provisions set out as a note under this section and section 201 of this title. For complete classification of title XIII to the Code, see Short Title of 2009 Amendment note set out under section 201 of this title and Tables.

Section 13101 of this Act, referred to in subsec. (c), means section 13101 of div. A of Pub. L. 111–5.

## EFFECTIVE DATE

Pub. L. 111–5, div. A, title XIII, §13423, Feb. 17, 2009, 123 Stat. 276, provided that: “Except as otherwise specifically provided, the provisions of part I [probably means part 1 (§§13401–13411) of subtitle D of title XIII of div. A of Pub. L. 111–5, enacting this part and amending sections 1320d–5 and 1320d–6 of this title] shall take effect on the date that is 12 months after the date of the enactment of this title [Feb. 17, 2009].”

<sup>1</sup> See References in Text note below.

<sup>2</sup> So in original. Section 300jj–12 of this title was enacted on Feb. 17, 2009.

**§ 17932. Notification in the case of breach****(a) In general**

A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

**(b) Notification of covered entity by business associate**

A business associate of a covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify the covered entity of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

**(c) Breaches treated as discovered**

For purposes of this section, a breach shall be treated as discovered by a covered entity or by a business associate as of the first day on which such breach is known to such entity or associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

**(d) Timeliness of notification****(1) In general**

Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

**(2) Burden of proof**

The covered entity involved (or business associate involved in the case of a notification required under subsection (b)), shall have the burden of demonstrating that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

**(e) Methods of notice****(1) Individual notice**

Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified

as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) In the case in which there is insufficient, or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on the home page of the Web site of the covered entity involved or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

(C) In any case deemed by the covered entity involved to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity, in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

**(2) Media notice**

Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

**(3) Notice to Secretary**

Notice shall be provided to the Secretary by covered entities of unsecured protected health information that has been acquired or disclosed in a breach. If the breach was with respect to 500 or more individuals than<sup>1</sup> such notice must be provided immediately. If the breach was with respect to less than 500 individuals, the covered entity may maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.

**(4) Posting on HHS public website**

The Secretary shall make available to the public on the Internet website of the Department of Health and Human Services a list that identifies each covered entity involved in a breach described in subsection (a) in which the unsecured protected health information of more than 500 individuals is acquired or disclosed.

<sup>1</sup> So in original. Probably should be "then".

**(f) Content of notification**

Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

(2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

(3) The steps individuals should take to protect themselves from potential harm resulting from the breach.

(4) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

**(g) Delay of notification authorized for law enforcement purposes**

If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

**(h) Unsecured protected health information****(1) Definition****(A) In general**

Subject to subparagraph (B), for purposes of this section, the term “unsecured protected health information” means protected health information that is not secured through the use of a technology or methodology specified by the Secretary in the guidance issued under paragraph (2).

**(B) Exception in case timely guidance not issued**

In the case that the Secretary does not issue guidance under paragraph (2) by the date specified in such paragraph, for purposes of this section, the term “unsecured protected health information” shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

**(2) Guidance**

For purposes of paragraph (1) and section 17937(f)(3) of this title, not later than the date that is 60 days after February 17, 2009, the Secretary shall, after consultation with stakeholders, issue (and annually update) guidance

specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, including the use of standards developed under section 300jj-12(b)(2)(B)(vi) of this title, as added by section 13101 of this Act.

**(i) Report to Congress on breaches****(1) In general**

Not later than 12 months after February 17, 2009, and annually thereafter, the Secretary shall prepare and submit to the Committee on Finance and the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Ways and Means and the Committee on Energy and Commerce of the House of Representatives a report containing the information described in paragraph (2) regarding breaches for which notice was provided to the Secretary under subsection (e)(3).

**(2) Information**

The information described in this paragraph regarding breaches specified in paragraph (1) shall include—

(A) the number and nature of such breaches; and

(B) actions taken in response to such breaches.

**(j) Regulations; effective date**

To carry out this section, the Secretary of Health and Human Services shall promulgate interim final regulations by not later than the date that is 180 days after February 17, 2009. The provisions of this section shall apply to breaches that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

(Pub. L. 111-5, div. A, title XIII, §13402, Feb. 17, 2009, 123 Stat. 260.)

## REFERENCES IN TEXT

Section 13101 of this Act, referred to in subsec. (h)(2), means section 13101 of div. A of Pub. L. 111-5.

**§ 17933. Education on health information privacy****(a) Regional office privacy advisors**

Not later than 6 months after February 17, 2009, the Secretary shall designate an individual in each regional office of the Department of Health and Human Services to offer guidance and education to covered entities, business associates, and individuals on their rights and responsibilities related to Federal privacy and security requirements for protected health information.

**(b) Education initiative on uses of health information**

Not later than 12 months after February 17, 2009, the Office for Civil Rights within the Department of Health and Human Services shall develop and maintain a multi-faceted national education initiative to enhance public transparency regarding the uses of protected health information, including programs to educate individuals about the potential uses of their protected health information, the effects of such uses, and the rights of individuals with respect

to such uses. Such programs shall be conducted in a variety of languages and present information in a clear and understandable manner.

(Pub. L. 111–5, div. A, title XIII, §13403, Feb. 17, 2009, 123 Stat. 263.)

**§ 17934. Application of privacy provisions and penalties to business associates of covered entities**

**(a) Application of contract requirements**

In the case of a business associate of a covered entity that obtains or creates protected health information pursuant to a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations, with such covered entity, the business associate may use and disclose such protected health information only if such use or disclosure, respectively, is in compliance with each applicable requirement of section 164.504(e) of such title. The additional requirements of this subchapter that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to such a business associate and shall be incorporated into the business associate agreement between the business associate and the covered entity.

**(b) Application of knowledge elements associated with contracts**

Section 164.504(e)(1)(ii) of title 45, Code of Federal Regulations, shall apply to a business associate described in subsection (a), with respect to compliance with such subsection, in the same manner that such section applies to a covered entity, with respect to compliance with the standards in sections 164.502(e) and 164.504(e) of such title, except that in applying such section 164.504(e)(1)(ii) each reference to the business associate, with respect to a contract, shall be treated as a reference to the covered entity involved in such contract.

**(c) Application of civil and criminal penalties**

In the case of a business associate that violates any provision of subsection (a) or (b), the provisions of sections 1176 and 1177 of the Social Security Act (42 U.S.C. 1320d–5, 1320d–6) shall apply to the business associate with respect to such violation in the same manner as such provisions apply to a person who violates a provision of part C of title XI of such Act [42 U.S.C. 1320d et seq.].

(Pub. L. 111–5, div. A, title XIII, §13404, Feb. 17, 2009, 123 Stat. 264.)

REFERENCES IN TEXT

This subchapter, referred to in subsec. (a), was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

The Social Security Act, referred to in subsec. (c), is act Aug. 14, 1935, ch. 531, 49 Stat. 620. Part C of title XI of the Act is classified generally to part C (§1320d et seq.) of subchapter XI of chapter 7 of this title. For complete classification of this Act to the Code, see section 1305 of this title and Tables.

**§ 17935. Restrictions on certain disclosures and sales of health information; accounting of certain protected health information disclosures; access to certain information in electronic format**

**(a) Requested restrictions on certain disclosures of health information**

In the case that an individual requests under paragraph (a)(1)(i)(A) of section 164.522 of title 45, Code of Federal Regulations, that a covered entity restrict the disclosure of the protected health information of the individual, notwithstanding paragraph (a)(1)(ii) of such section, the covered entity must comply with the requested restriction if—

(1) except as otherwise required by law, the disclosure is to a health plan for purposes of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and

(2) the protected health information pertains solely to a health care item or service for which the health care provider involved has been paid out of pocket in full.

**(b) Disclosures required to be limited to the limited data set or the minimum necessary**

**(1) In general**

**(A) In general**

Subject to subparagraph (B), a covered entity shall be treated as being in compliance with section 164.502(b)(1) of title 45, Code of Federal Regulations, with respect to the use, disclosure, or request of protected health information described in such section, only if the covered entity limits such protected health information, to the extent practicable, to the limited data set (as defined in section 164.514(e)(2) of such title) or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request, respectively.

**(B) Guidance**

Not later than 18 months after February 17, 2009, the Secretary shall issue guidance on what constitutes “minimum necessary” for purposes of subpart E of part 164 of title 45, Code of Federal Regulation.<sup>1</sup> In issuing such guidance the Secretary shall take into consideration the guidance under section 17953(c) of this title and the information necessary to improve patient outcomes and to detect, prevent, and manage chronic disease.

**(C) Sunset**

Subparagraph (A) shall not apply on and after the effective date on which the Secretary issues the guidance under subparagraph (B).

**(2) Determination of minimum necessary**

For purposes of paragraph (1), in the case of the disclosure of protected health information, the covered entity or business associate disclosing such information shall determine what constitutes the minimum necessary to accomplish the intended purpose of such disclosure.

<sup>1</sup> So in original. Probably should be “Regulations.”

**(3) Application of exceptions**

The exceptions described in section 164.502(b)(2) of title 45, Code of Federal Regulations, shall apply to the requirement under paragraph (1) as of the effective date described in section 13423<sup>2</sup> in the same manner that such exceptions apply to section 164.502(b)(1) of such title before such date.

**(4) Rule of construction**

Nothing in this subsection shall be construed as affecting the use, disclosure, or request of protected health information that has been de-identified.

**(c) Accounting of certain protected health information disclosures required if covered entity uses electronic health record****(1) In general**

In applying section 164.528 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information—

(A) the exception under paragraph (a)(1)(i) of such section shall not apply to disclosures through an electronic health record made by such entity of such information; and

(B) an individual shall have a right to receive an accounting of disclosures described in such paragraph of such information made by such covered entity during only the three years prior to the date on which the accounting is requested.

**(2) Regulations**

The Secretary shall promulgate regulations on what information shall be collected about each disclosure referred to in paragraph (1), not later than 6 months after the date on which the Secretary adopts standards on accounting for disclosure described in the section 300jj-12(b)(2)(B)(iv) of this title, as added by section 13101.<sup>2</sup> Such regulations shall only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures.

**(3) Process**

In response to an<sup>3</sup> request from an individual for an accounting, a covered entity shall elect to provide either an—

(A) accounting, as specified under paragraph (1), for disclosures of protected health information that are made by such covered entity and by a business associate acting on behalf of the covered entity; or

(B) accounting, as specified under paragraph (1), for disclosures that are made by such covered entity and provide a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

<sup>2</sup> See References in Text note below.

<sup>3</sup> So in original. Probably should be “a”.

A business associate included on a list under subparagraph (B) shall provide an accounting of disclosures (as required under paragraph (1) for a covered entity) made by the business associate upon a request made by an individual directly to the business associate for such an accounting.

**(4) Effective date****(A) Current users of electronic records**

In the case of a covered entity insofar as it acquired an electronic health record as of January 1, 2009, paragraph (1) shall apply to disclosures, with respect to protected health information, made by the covered entity from such a record on and after January 1, 2014.

**(B) Others**

In the case of a covered entity insofar as it acquires an electronic health record after January 1, 2009, paragraph (1) shall apply to disclosures, with respect to protected health information, made by the covered entity from such record on and after the later of the following:

(i) January 1, 2011; or

(ii) the date that it acquires an electronic health record.

**(C) Later date**

The Secretary may set an effective date that is later than<sup>4</sup> the date specified under subparagraph (A) or (B) if the Secretary determines that such later date is necessary, but in no case may the date specified under—

(i) subparagraph (A) be later than 2016; or

(ii) subparagraph (B) be later than 2013.

**(d) Prohibition on sale of electronic health records or protected health information****(1) In general**

Except as provided in paragraph (2), a covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual unless the covered entity obtained from the individual, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization that includes, in accordance with such section, a specification of whether the protected health information can be further exchanged for remuneration by the entity receiving protected health information of that individual.

**(2) Exceptions**

Paragraph (1) shall not apply in the following cases:

(A) The purpose of the exchange is for public health activities (as described in section 164.512(b) of title 45, Code of Federal Regulations).

(B) The purpose of the exchange is for research (as described in sections 164.501 and 164.512(i) of title 45, Code of Federal Regulations) and the price charged reflects the costs of preparation and transmittal of the data for such purpose.

<sup>4</sup> So in original. Probably should be “than”.

(C) The purpose of the exchange is for the treatment of the individual, subject to any regulation that the Secretary may promulgate to prevent protected health information from inappropriate access, use, or disclosure.

(D) The purpose of the exchange is the health care operation specifically described in subparagraph (iv) of paragraph (6) of the definition of healthcare operations in section 164.501 of title 45, Code of Federal Regulations.

(E) The purpose of the exchange is for remuneration that is provided by a covered entity to a business associate for activities involving the exchange of protected health information that the business associate undertakes on behalf of and at the specific request of the covered entity pursuant to a business associate agreement.

(F) The purpose of the exchange is to provide an individual with a copy of the individual's protected health information pursuant to section 164.524 of title 45, Code of Federal Regulations.

(G) The purpose of the exchange is otherwise determined by the Secretary in regulations to be similarly necessary and appropriate as the exceptions provided in subparagraphs (A) through (F).

### (3) Regulations

Not later than 18 months after February 17, 2009, the Secretary shall promulgate regulations to carry out this subsection. In promulgating such regulations, the Secretary—

(A) shall evaluate the impact of restricting the exception described in paragraph (2)(A) to require that the price charged for the purposes described in such paragraph reflects the costs of the preparation and transmittal of the data for such purpose, on research or public health activities, including those conducted by or for the use of the Food and Drug Administration; and

(B) may further restrict the exception described in paragraph (2)(A) to require that the price charged for the purposes described in such paragraph reflects the costs of the preparation and transmittal of the data for such purpose, if the Secretary finds that such further restriction will not impede such research or public health activities.

### (4) Effective date

Paragraph (1) shall apply to exchanges occurring on or after the date that is 6 months after the date of the promulgation of final regulations implementing this subsection.

### (e) Access to certain information in electronic format

In applying section 164.524 of title 45, Code of Federal Regulations, in the case that a covered entity uses or maintains an electronic health record with respect to protected health information of an individual—

(1) the individual shall have a right to obtain from such covered entity a copy of such information in an electronic format and, if the individual chooses, to direct the covered entity to transmit such copy directly to an en-

tity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific; and

(2) notwithstanding paragraph (c)(4) of such section, any fee that the covered entity may impose for providing such individual with a copy of such information (or a summary or explanation of such information) if such copy (or summary or explanation) is in an electronic form shall not be greater than the entity's labor costs in responding to the request for the copy (or summary or explanation).

(Pub. L. 111-5, div. A, title XIII, §13405, Feb. 17, 2009, 123 Stat. 264.)

#### REFERENCES IN TEXT

Section 13423, referred to in subsec. (b)(3), means section 13423 of div. A of Pub. L. 111-5, which is set out as an Effective Date note under section 17931 of this title.

Section 13101, referred to in subsec. (c)(2), means section 13101 of div. A of Pub. L. 111-5.

### § 17936. Conditions on certain contacts as part of health care operations

#### (a) Marketing

##### (1) In general

A communication by a covered entity or business associate that is about a product or service and that encourages recipients of the communication to purchase or use the product or service shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations, unless the communication is made as described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of such title.

##### (2) Payment for certain communications

A communication by a covered entity or business associate that is described in subparagraph (i), (ii), or (iii) of paragraph (1) of the definition of marketing in section 164.501 of title 45, Code of Federal Regulations, shall not be considered a health care operation for purposes of subpart E of part 164 of title 45, Code of Federal Regulations if the covered entity receives or has received direct or indirect payment in exchange for making such communication, except where—

(A)(i) such communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and

(ii) any payment received by such covered entity in exchange for making a communication described in clause (i) is reasonable in amount;

(B) each of the following conditions apply—

(i) the communication is made by the covered entity; and

(ii) the covered entity making such communication obtains from the recipient of the communication, in accordance with section 164.508 of title 45, Code of Federal Regulations, a valid authorization (as described in paragraph (b) of such section) with respect to such communication; or

(C) each of the following conditions apply—

(i) the communication is made by a business associate on behalf of the covered entity; and

(ii) the communication is consistent with the written contract (or other written arrangement described in section 164.502(e)(2) of such title) between such business associate and covered entity.

**(3) Reasonable in amount defined**

For purposes of paragraph (2), the term “reasonable in amount” shall have the meaning given such term by the Secretary by regulation.

**(4) Direct or indirect payment**

For purposes of paragraph (2), the term “direct or indirect payment” shall not include any payment for treatment (as defined in section 164.501 of title 45, Code of Federal Regulations) of an individual.

**(b) Opportunity to opt out of fundraising**

The Secretary shall by rule provide that any written fundraising communication that is a healthcare operation as defined under section 164.501 of title 45, Code of Federal Regulations, shall, in a clear and conspicuous manner, provide an opportunity for the recipient of the communications to elect not to receive any further such communication. When an individual elects not to receive any further such communication, such election shall be treated as a revocation of authorization under section 164.508 of title 45, Code of Federal Regulations.

**(c) Effective date**

This section shall apply to written communications occurring on or after the effective date specified under section 13423.<sup>1</sup>

(Pub. L. 111–5, div. A, title XIII, §13406, Feb. 17, 2009, 123 Stat. 268.)

REFERENCES IN TEXT

Section 13423, referred to in subsec. (c), means section 13423 of div. A of Pub. L. 111–5, which is set out as an Effective Date note under section 17931 of this title.

**§ 17937. Temporary breach notification requirement for vendors of personal health records and other non-HIPAA covered entities**

**(a) In general**

In accordance with subsection (c), each vendor of personal health records, following the discovery of a breach of security of unsecured PHR identifiable health information that is in a personal health record maintained or offered by such vendor, and each entity described in clause (ii), (iii), or (iv) of section 17953(b)(1)(A) of this title, following the discovery of a breach of security of such information that is obtained through a product or service provided by such entity, shall—

(1) notify each individual who is a citizen or resident of the United States whose unsecured PHR identifiable health information was acquired by an unauthorized person as a result of such a breach of security; and

(2) notify the Federal Trade Commission.

**(b) Notification by third party service providers**

A third party service provider that provides services to a vendor of personal health records or to an entity described in clause (ii), (iii),<sup>1</sup> or (iv) of section 17953(b)(1)(A) of this title in connection with the offering or maintenance of a personal health record or a related product or service and that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information in such a record as a result of such services shall, following the discovery of a breach of security of such information, notify such vendor or entity, respectively, of such breach. Such notice shall include the identification of each individual whose unsecured PHR identifiable health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

**(c) Application of requirements for timeliness, method, and content of notifications**

Subsections (c), (d), (e), and (f) of section 17932 of this title shall apply to a notification required under subsection (a) and a vendor of personal health records, an entity described in subsection (a) and a third party service provider described in subsection (b), with respect to a breach of security under subsection (a) of unsecured PHR identifiable health information in such records maintained or offered by such vendor, in a manner specified by the Federal Trade Commission.

**(d) Notification of the Secretary**

Upon receipt of a notification of a breach of security under subsection (a)(2), the Federal Trade Commission shall notify the Secretary of such breach.

**(e) Enforcement**

A violation of subsection (a) or (b) shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 57a(a)(1)(B) of title 15 regarding unfair or deceptive acts or practices.

**(f) Definitions**

For purposes of this section:

**(1) Breach of security**

The term “breach of security” means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual.

**(2) PHR identifiable health information**

The term “PHR identifiable health information” means individually identifiable health information, as defined in section 1320d(6) of this title, and includes, with respect to an individual, information—

(A) that is provided by or on behalf of the individual; and

(B) that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

<sup>1</sup> See References in Text note below.

<sup>1</sup> So in original. The period probably should be a comma.

**(3) Unsecured PHR identifiable health information**

**(A) In general**

Subject to subparagraph (B), the term “unsecured PHR identifiable health information” means PHR identifiable health information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under section 17932(h)(2) of this title.

**(B) Exception in case timely guidance not issued**

In the case that the Secretary does not issue guidance under section 17932(h)(2) of this title by the date specified in such section, for purposes of this section, the term “unsecured PHR identifiable health information” shall mean PHR identifiable health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and that is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

**(g) Regulations; effective date; sunset**

**(1) Regulations; effective date**

To carry out this section, the Federal Trade Commission shall promulgate interim final regulations by not later than the date that is 180 days after February 17, 2009. The provisions of this section shall apply to breaches of security that are discovered on or after the date that is 30 days after the date of publication of such interim final regulations.

**(2) Sunset**

If Congress enacts new legislation establishing requirements for notification in the case of a breach of security, that apply to entities that are not covered entities or business associates, the provisions of this section shall not apply to breaches of security discovered on or after the effective date of regulations implementing such legislation.

(Pub. L. 111–5, div. A, title XIII, §13407, Feb. 17, 2009, 123 Stat. 269.)

**§ 17938. Business associate contracts required for certain entities**

Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity (or its business associate) and that requires access on a routine basis to such protected health information, such as a Health Information Exchange Organization, Regional Health Information Organization, E-prescribing Gateway, or each vendor that contracts with a covered entity to allow that covered entity to offer a personal health record to patients as part of its electronic health record, is required to enter into a written contract (or other written arrangement) described in section 164.502(e)(2) of title 45, Code of Federal Regulations and a written contract (or other arrangement) described in section 164.308(b) of such title, with such entity and

shall be treated as a business associate of the covered entity for purposes of the provisions of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009.

(Pub. L. 111–5, div. A, title XIII, §13408, Feb. 17, 2009, 123 Stat. 271.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111–5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

**§ 17939. Improved enforcement**

**(a) In general**

**(1) Omitted**

**(2) Enforcement under Social Security Act**

Any violation by a covered entity under thus<sup>1</sup> subchapter is subject to enforcement and penalties under section<sup>2</sup> 1176 and 1177 of the Social Security Act [42 U.S.C. 1320d–5, 1320d–6].

**(b) Effective date; regulations**

(1) The amendments made by subsection (a) shall apply to penalties imposed on or after the date that is 24 months after February 17, 2009.

(2) Not later than 18 months after February 17, 2009, the Secretary of Health and Human Services shall promulgate regulations to implement such amendments.

**(c) Distribution of certain civil monetary penalties collected**

**(1) In general**

Subject to the regulation promulgated pursuant to paragraph (3), any civil monetary penalty or monetary settlement collected with respect to an offense punishable under this subchapter or section 1176 of the Social Security Act (42 U.S.C. 1320d–5) insofar as such section relates to privacy or security shall be transferred to the Office for Civil Rights of the Department of Health and Human Services to be used for purposes of enforcing the provisions of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009.

**(2) GAO report**

Not later than 18 months after February 17, 2009, the Comptroller General shall submit to the Secretary a report including recommendations for a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

**(3) Establishment of methodology to distribute percentage of CMPS collected to harmed individuals**

Not later than 3 years after February 17, 2009, the Secretary shall establish by regula-

<sup>1</sup> So in original. Probably should be “this”.

<sup>2</sup> So in original. Probably should be “sections”.

tion and based on the recommendations submitted under paragraph (2), a methodology under which an individual who is harmed by an act that constitutes an offense referred to in paragraph (1) may receive a percentage of any civil monetary penalty or monetary settlement collected with respect to such offense.

**(4) Application of methodology**

The methodology under paragraph (3) shall be applied with respect to civil monetary penalties or monetary settlements imposed on or after the effective date of the regulation.

**(d) Tiered increase in amount of civil monetary penalties**

**(1) to (3) Omitted**

**(4) Effective date**

The amendments made by this subsection shall apply to violations occurring after February 17, 2009.

**(e) Enforcement through State attorneys general**

**(1), (2) Omitted**

**(3) Effective date**

The amendments made by this subsection shall apply to violations occurring after February 17, 2009.

(Pub. L. 111-5, div. A, title XIII, §13410, Feb. 17, 2009, 123 Stat. 271.)

REFERENCES IN TEXT

This subchapter, referred to in subsecs. (a)(2) and (c)(1), was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

For reference to “the amendments made by subsection (a)” in subsec. (b)(1) and “the amendments made by this subsection” in subsecs. (d)(4) and (e)(3), see Codification note below.

CODIFICATION

Section is comprised of section 13410 of Pub. L. 111-5. Subsecs. (a)(1), (d)(1)–(3), (e)(1), (2), and (f) of section 13410 of Pub. L. 111-5 amended section 1320d-5 of this title.

**§ 17940. Audits**

The Secretary shall provide for periodic audits to ensure that covered entities and business associates that are subject to the requirements of this subchapter and subparts C and E of part 164 of title 45, Code of Federal Regulations, as such provisions are in effect as of February 17, 2009, comply with such requirements.

(Pub. L. 111-5, div. A, title XIII, §13411, Feb. 17, 2009, 123 Stat. 276.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

PART B—RELATIONSHIP TO OTHER LAWS; REGULATORY REFERENCES; EFFECTIVE DATE; REPORTS

**§ 17951. Relationship to other laws**

**(a) Application of HIPAA State preemption**

Section 1178 of the Social Security Act (42 U.S.C. 1320d-7) shall apply to a provision or requirement under this subchapter in the same manner that such section applies to a provision or requirement under part C of title XI of such Act [42 U.S.C. 1320d et seq.] or a standard or implementation specification adopted or established under sections 1172 through 1174 of such Act [42 U.S.C. 1320d-1 to 1320d-3].

**(b) Health Insurance Portability and Accountability Act of 1996**

The standards governing the privacy and security of individually identifiable health information promulgated by the Secretary under sections 262(a) and 264 of the Health Insurance Portability and Accountability Act of 1996 shall remain in effect to the extent that they are consistent with this subchapter. The Secretary shall by rule amend such Federal regulations as required to make such regulations consistent with this subchapter.

**(c) Construction**

Nothing in this subchapter shall constitute a waiver of any privilege otherwise applicable to an individual with respect to the protected health information of such individual.

(Pub. L. 111-5, div. A, title XIII, §13421, Feb. 17, 2009, 123 Stat. 276.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this subchapter. For complete classification of subtitle D to the Code, see Tables.

The Social Security Act, referred to in subsec. (a), is act Aug. 14, 1935, ch. 531, 49 Stat. 620. Part C of title XI of the Act is classified generally to part C (§1320d et seq.) of subchapter XI of chapter 7 of this title. For complete classification of this Act to the Code, see section 1305 of this title and Tables.

The Health Insurance Portability and Accountability Act of 1996, referred to in subsec. (b), is Pub. L. 104-191, Aug. 21, 1996, 110 Stat. 1936. Section 262(a) of the Act enacted sections 1320d to 1320d-8 of this title. Section 264 of the Act is set out as a note under section 1320d-2 of this title. For complete classification of this Act to the Code, see Short Title of 1996 Amendments note set out under section 201 of this title and Tables.

**§ 17952. Regulatory references**

Each reference in this subchapter to a provision of the Code of Federal Regulations refers to such provision as in effect on February 17, 2009 (or to the most recent update of such provision).

(Pub. L. 111-5, div. A, title XIII, §13422, Feb. 17, 2009, 123 Stat. 276.)

REFERENCES IN TEXT

This subchapter, referred to in text, was in the original “this subtitle”, meaning subtitle D (§13400 et seq.) of title XIII of div. A of Pub. L. 111-5, Feb. 17, 2009, 123 Stat. 258, which is classified principally to this sub-